REMARKS

Claims 1, 4, 11, 19, 25, 30, 36, 41, 42, 47, and 48 have been amended. Claims 2, 3, 27, 31, and 43 have been canceled. Claims 1, 4-26, 28-30, 32-42, and 44-48 are currently pending in the application. In view of the following remarks, Applicant respectfully requests withdrawal of the rejections and forwarding of the application onto issuance.

The § 102 Rejections

Claims 1-10 and 25-48 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,757,919 to Herbert et al (hereinafter "Herbert").

The § 103 Rejections

Claims 11-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Herbert in view of U.S. Patent No. 5,628,023 to Bryant et al. (hereinafter "Bryant").

Claims 19-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Herbert in view of U.S. Patent No. 6,003,117 to Buer et al. (hereinafter "Buer").

Claims 1 and 4-10

As amended, **claim 1** recites, in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory, a computer-implemented method of protecting information comprising [emphasis added]:

- creating a key and page locking the key in the physical memory, wherein creating the key comprises creating the key during ***system***

boot up, wherein ***different*** keys can be created during ***different*** system boot ups;

- encrypting information using the key; and
- paging out, to the page file, the encrypted information.

In making out the rejection of former claim 3, which subject matter is now incorporated into claim 1, the Office argues that Herbert teaches a method for creating a key during system boot up and cites to column 2, lines 45-52, reproduced below, for support:

> The flash memory is used for long-term storage of secret information, and a portion thereof may be allocated to applications running in the secure environment Additionally, in one embodiment, the real time kernel for secure processor 16 is stored in the flash memory. This allows all basic operations to be performed without external intervention (active or passive), and improves performance as compared to moving the kernel through the security services described herein.

Applicant respectfully submits that the excerpt cited by the Office does ***not*** teach that a key is created during ***system boot up***. Applicant directs the Office's attention to column 4, lines 7-25, and column 6, lines 59-60, which teach that Herbert's key is generated ***at the time of software installation***. Those excerpts are reproduced below [emphasis added]:

> At some time, software must be installed in the secure environment. Such "off the shelf" software will, of course, not be encrypted in the manner used within the secure environment. It will typically have a digital signature which can be used to verify the authenticity of the software being installed if digital signature verification is a supported function within the secure environment. ***FIG. 3 shows a flowchart of installation of a program in the secure system. At functional block 120, a key is generated and initialization vector [IV] is generated for an application to be installed.*** Key generation can be accomplished using the random number generator which generates random bits. Random bits are collected until the desired key length is reached. In one embodiment, the random number generator has a thirty-two bit output register. The processor 16 reads the register a number of times necessary to collect enough random

> bits for a full key. Keys can be generated with one key for each application, i.e. all code pages and data pages associated with one application share the same key. *Col. 4, lines 7-25.*
>
> As discussed above, the encryption key and IV are generated ***at the time of installation.*** *Col. 6, lines 59-60.*

Applicant respectfully submits that Herbert ***specifically teaches*** that its key is created ***at the time of software installation***. Furthermore, Applicant has amended claim 1 to clarify that ***different*** keys can be created during ***different*** system boot ups. In contrast, Herbert appears to utilize the ***same*** key(s) created for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Claims 4-10 depend either directly or indirectly from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claims 11-18

As amended, **claim 11** recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- creating a key during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups;
- page-locking the key in main memory;
- restricting access to the page-locked key to only the operating system kernel;
- calling the operating system kernel to encrypt information;
- accessing the page-locked key with the operating system kernel; and

- using the operating system kernel to encrypt the information with the page-locked key.

In making out the rejection of former claim 3, which subject matter is now incorporated into claim 11, the Office argues that Herbert teaches a method for creating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is generated ***at the time of software installation***. Furthermore, Applicant has amended claim 11 to clarify that ***different*** keys can be created during ***different*** system boot ups. In contrast, Herbert appears to utilize the ***same*** key(s) created for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Claims 12-18 depend either directly or indirectly from claim 11 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 11, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claims 19-24

As amended, **claim 19** recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of handling encrypted information comprising [emphasis added]:

- accessing encrypted information in the page file; and
- decrypting the encrypted information with a key created during ***system boot up***, wherein ***different*** keys can be created during

different system boot ups and wherein the key is page-locked in the main memory.

In making out the rejection of former claim 3, which subject matter is now incorporated into claim 19, the Office argues that Herbert teaches a method for creating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is created ***at the time of software installation***. Furthermore, Applicant has amended claim 19 to clarify that ***different*** keys can be created during ***different*** system boot ups. In contrast, Herbert appears to utilize the ***same*** key(s) created for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Claims 20-24 depend either directly or indirectly from claim 19 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 19, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claims 25-26 and 28-29

As amended, **claim 25** recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- allocating a non-pageable page of main memory during ***system boot***;
- generating a random key, wherein ***different*** keys can be generated during ***different*** system boots; and

- storing the random key in the non-pageable page of main memory, the random key being configured for use by the operating system to encrypt information that might be paged out to the page file.

In making out the rejection of former claim 27, which subject matter is now incorporated into claim 25, the Office argues that Herbert teaches a method for generating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is generated ***at the time of software installation***. Furthermore, Applicant has amended claim 25 to clarify that ***different*** keys can be generated during ***different*** system boots. In contrast, Herbert appears to utilize the ***same*** key(s) generated for a given software application across ***multiple*** system boots. Accordingly, for at least these reasons, this claim is allowable.

Claims 26 and 28-29 depend either directly or indirectly from claim 25 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 25, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claims 30 and 32-35

As amended, **claim 30** recites, in an operating system having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- generating at least one non-pageable random key by using a random key generation process during ***system boot up***, wherein ***different*** keys can be generated during ***different*** system boot ups;

- encrypting at least one selected block of information in the main memory with a software component that uses the at least one random key for encryption;
- transferring the one encrypted block of information to the secondary storage;
- decrypting the one encrypted block of information with the software component that uses the at least one random key for decryption; and
- placing the decrypted block of information in the main memory.

In making out the rejection of former claim 31, which subject matter is now incorporated into claim 30, the Office argues that Herbert teaches a method for generating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is generated ***at the time of software installation***. Furthermore, Applicant has amended claim 30 to clarify that ***different*** keys can be generated during ***different system boot ups***. In contrast, Herbert appears to utilize the ***same*** key(s) generated for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Claims 32-35 depend either directly or indirectly from claim 30 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 30, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claims 36-40

As amended, **claim 36** recites a system for use in protecting pageable information comprising [emphasis added]:

- a memory having pageable and non-pageable pages; and

- at least one key created during ***system boot*** and stored in the memory in a non-pageable page, the key being configured for use in encrypting pageable information, wherein ***different*** keys can be created during ***different*** system boots.

In making out the rejection of former claim 3, which subject matter is now incorporated into claim 36, the Office argues that Herbert teaches a method for creating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is created ***at the time of software installation***. Furthermore, Applicant has amended claim 36 to clarify that ***different*** keys can be created during ***different*** system boot ups. In contrast, Herbert appears to utilize the ***same*** key(s) created for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Claims 37-40 depend either directly or indirectly from claim 36 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 36, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claim 41

As amended, **claim 41** recites a computer program embodied on one or more computer-readable media, the program comprising [emphasis added]:

- creating a key and page locking the key in main memory of a computer, wherein creating the key comprises creating the key during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups;
- encrypting information with the key;
- paging out, to secondary storage, the encrypted information;
- accessing the encrypted information in the secondary storage; and

- decrypting the encrypted information with the key that is page-locked in the main memory.

In making out the rejection of former claim 3, which subject matter is now incorporated into claim 41, the Office argues that Herbert teaches a method for creating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is created ***at the time of software installation***. Furthermore, Applicant has amended claim 41 to clarify that ***different*** keys can be created during ***different*** system boot ups. In contrast, Herbert appears to utilize the ***same*** key(s) created for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Claims 42 and 44-46

As amended, **claim 42** recites a programmable computer comprising [emphasis added]:

- a processor;
- main memory for holding information;
- secondary storage for receiving information that is temporarily transferred out of the main memory;
- the computer being programmed with computer-readable instructions which, when executed by the processor, cause the computer to:
  - generate a key during ***system boot up***, wherein ***different*** keys can be generated during ***different*** system boot ups;
  - page lock the key in the main memory;
  - encrypt information that is to be transferred to the secondary storage with the key;
  - transfer the encrypted information to the secondary storage; and
  - decrypt the encrypted information with a key that is locked in the main memory.

In making out the rejection of former claim 31, which subject matter is now incorporated into claim 42, the Office argues that Herbert teaches a method for generating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is generated ***at the time of software installation***. Furthermore, Applicant has amended claim 42 to clarify that ***different*** keys can be generated during ***different*** system boot ups. In contrast, Herbert appears to utilize the ***same*** key(s) generated for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Claims 44-46 depend either directly or indirectly from claim 42 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 42, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claim 47

As amended, **claim 47** recites one or more ***application programming interfaces*** embodied on one or more computer-readable media for execution on a computer in conjunction with a paging operating system having main memory for holding information and a page file for receiving information that is paged out from the main memory, comprising [emphasis added]:

- an interface method for generating a key during ***system boot up***, wherein ***different*** keys can be generated during ***different*** system boot ups;
- an interface method for page locking the key in the main memory,
- an interface method for encrypting pageable information with the key; and

- an interface method for decrypting encrypted information that is contained in the page file.

In making out the rejection of former claim 31, which subject matter is similar to the amended language of claim 47, the Office argues that Herbert teaches a method for generating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is generated ***at the time of software installation***. Furthermore, Applicant has amended claim 47 to clarify that ***different*** keys can be generated during ***different*** system boot ups. In contrast, Herbert appears to utilize the ***same*** key(s) generated for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Claim 48

As amended, **claim 48** recites an application programming interface embodied on a computer-readable medium for execution on a computer in conjunction with a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, comprising a method for setting an attribute on a page of main memory, the attribute designating that the page must be encrypted with a key created during ***system boot up*** and page-locked in the main memory prior to the page being paged out to the page file, wherein ***different*** keys can be created during ***different*** system boot ups.

In making out the rejection of former claim 3, which subject matter is now incorporated into claim 48, the Office argues that Herbert teaches a method for creating a key during system boot up and cites to column 2, lines 45-52, reproduced above, for support.

As discussed above, Applicant respectfully submits that Herbert ***specifically teaches*** that its key is created ***at the time of software installation***. Furthermore, Applicant has amended claim 48 to clarify that ***different*** keys can be created during ***different*** system boot ups. In contrast, Herbert appears to utilize the ***same*** key(s) created for a given software application across ***multiple*** system boot ups. Accordingly, for at least these reasons, this claim is allowable.

Conclusion

Applicant respectfully submits that all of the claims are in condition for allowance. Accordingly, Applicant requests that a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant requests that the undersigned be contacted for the purpose of scheduling an interview.

Respectfully submitted,

Dated: 11/15/04

By: Reg. No. 38605 for Rob Cottle
Rob R. Cottle
Reg. No. 52,772
(509) 324-9256 ext. 247